IBM.Pre.C1000-018.by.VCEplus.60q - DEMO

Exam A

QUESTION 1 Which use case type is appropriate for VPN log sources?
(Choose two.)

A. Advanced Persistent Threat (APT)
B. Insider Threat
C. Critical Data Protection
D. Securing the Cloud

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/dsm?topic=management-threat-use-cases-by-log-source-type

QUESTION 2

What is displayed in the status bar of the Log Activity tab when streaming events?

A. Average number of results that are received per second.
B. Average number of results that are received per minute.
C. Accumulated number of results that are received per second.
D. Accumulated number of results that are received per minute.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Status bar
When streaming events, the status bar displays the average number of results that are received per second.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-log-activity-tab-overview

QUESTION 3

An analyst wants to analyze the long-term trending of data from a search.

Which chart would be used to display this data on a dashboard?

A. Bar Graph
B. Time Series chart
C. Pie Chart
D. Scatter Chart

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You could use a bar graph if you want to track change over time as long as the changes are significant.

Reference: https://www.statisticshowto.com/probability-and-statistics/descriptive-statistics/bar-chart-bar-graph-examples/

QUESTION 4
When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?

A. When the source is [local or remote]
B. When the destination is [local or remote]
C. When the event(s) were detected by one or more of [these log sources]
D. When an event matches all of the following [Rules or Building Blocks]

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5 Why would an analyst update host definition building blocks in QRadar?

A. To reduce false positives.
B. To narrow a search.
C. To stop receiving events from the host.
D. To close an Offense

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Building blocks to reduce the number of offenses that are generated by high volume traffic servers.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=phase-qradar-building-blocks

QUESTION 6 After working with an Offense, an analyst set the Offense as hidden. What does the analyst need to do to view the Offense at a later time?

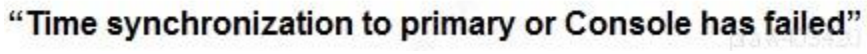
A. In the all Offenses view, at the top of the view, select “Show hidden” from the “Select an option” drop-down.
B. Search for all Offenses owned by the analyst.
C. Click Clear Filter next to the “Exclude Hidden Offenses”.
D. In the all Offenses view, select Actions, then select show hidden Offenses.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To clear the filter on the offense list, click Clear Filter next to the Exclude Hidden Offenses search parameter.

Reference: https://www.ibm.com/docs/fi/qradar-on-cloud?topic=actions-showing-hidden-offenses

QUESTION 7
What is the reason for this system notification?



“Time synchronization to primary or Console has failed”

A. Deny ntpdate communication on port 423. B.
Deny ntpdate communication on port 223. C.
Deny ntpdate communication on port 323.

D. Deny ntpdate communication on port 123.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
38750129 - Time synchronization to primary or Console has failed.
The managed host cannot synchronize with the console or the secondary HA appliance cannotsynchronize with the primary appliance. Administrators must allow ntpdatecommunication on port 123.

Reference: https://www.coursehero.com/file/p35nlom9/Process-exceeds-allowed-run-time-38750122-Process-takes-too-long-to-execute-The/

QUESTION 8
When an analyst sees the system notification “The appliance exceeded the EPS or FPM allocation within the last hour”, how does the analyst resolve this issue? (Choose two.)

A. Delete the volume of events and flows received in the last hour.
B. Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance.
C. Tune the system to reduce the volume of events and flows that enter the event pipeline.
D. Adjust the resource pool allocations to increase the EPS and FPM capacity for the appliance.
E. Tune the system to reduce the time window from 60 minutes to 30 minutes.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
User response
Adjust the license pool allocations to increase the EPS and FPM capacity for the appliance. Tune the system to reduce the volume of events and flows that enter the event pipeline.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=appliances-maximum-events-flows-reached

QUESTION 9
An analyst is encountering a large number of false positive results. Legitimate internal network traffic contains valid flows and events which are making it difficult to identify true security incidents.

What can the analyst do to reduce these false positive indicators?

A. Create X-Force rules to detect false positive events.
B. Create an anomaly rule to detect false positives and suppress the event.
C. Filter the network traffic to receive only security related events.
D. Modify rules and/or Building Block to suppress false positive activity.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10 What is the maximum time period for 3 subsequent events to be coalesced?

A. 10 minutes
B. 10 seconds
C. 5 minutes
D. 60 seconds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Event coalescing starts after three events have been found with matching properties within a 10 second window.

Reference: https://www.ibm.com/support/pages/qradar-how-does-coalescing-work-qradar

QUESTION 11
An analyst needs to create a new custom dashboard to view dashboard items that meet a particular requirement.

What are the main steps in the process?

A. Select New Dashboard and enter unique name, description, add items and save.
B. Select New Dashboard and copy name, add description, items and save.
C. Request the administrator to create the custom dashboard with required items.
D. Locate existing dashboard and modify to include indexed items required and save.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To create or edit your dashboards, log in as an administrator, click the Dashboards tab, and then click the gear icon. In edit mode, you can create new dashboards, add and remove widgets, edit display values in existing widgets, and reorder tabs.

Reference: https://documentation.solarwinds.com/en/success_center/tm/content/threatmonitor/tm-editdashboards.htm

QUESTION 12
What event information within an offense would provide the analyst with a deep insight as to how it was created?

A. Event Category
B. Event QID
C. Event Payload
D. Event Magnitude

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 How can analyst verify if any host in the deployment is vulnerable to CVE ID:
CVE-2010-000?

A. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: 2010-000
B. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: $CVE-2010000
C. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: $2010-000
D. Use the asset search feature, select vulnerability external reference from the list of search parameters, select CVE and then type: CVE-2010000

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=ap-searching-asset-profiles-from-asset-page-assets-tab

QUESTION 14
An analyst investigates an Offense that will need more research to outline what has occurred. The analyst marks a ‘Follow up’ flag on the Offense.

What happens to the Offense after it is tagged with a ‘Follow up’ flag?

A. Only the analyst issuing the follow up flag can now close the Offense.
B. New events or flows will not be applied to the Offense.
C. A flag icon is displayed for the Offense in the Offense view.
D. Other analysts in QRadar get an email to look at the Offense.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The offense now displays the follow-up icon in the Flag column.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=actions-marking-offense-follow-up

QUESTION 15
An analyst noticed that from a particular subnet (203.0.113.0/24), all IP addresses are simultaneously trying to reach out to the company’s publicly hosted FTP server. The analyst also noticed that this activity has resulted in a *Type B Superflow* on the Network Activity tab.

Under which category, should the analyst report this issue to the security administrator?

A. Syn Flood
B. Port Scan
C. Network Scan
D. DDoS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
An analyst is investigating an Offense and has found that the issue is that a firewall appears to be misconfigured and has permitted traffic that should be prevented to pass.

As part of the firewall rule change process, the analyst needs to send the offense details to the firewall team to demonstrate that the firewall permitted traffic that should have been blocked.

How would the analyst send the Offense summary to an email mailbox?

A. Find the CRE Event in the Log Activity tab, open the event detail and select ‘Email linked Offense details’ from the ‘Action’ menu.
B. Search for the events linked to the Offense in the Log Activity tab; Select all events and copy them using CTRL-C then paste into an email client.
C. Open the Offense in the Offenses tab, select ‘Email’ from the ‘Action’ menu item and, optionally, add some extra information.D. Identify the Offense in the Offense list, right click on the Offense and select ‘Custom Action Script’; ‘Offense Mailer’

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which statement about False Positive Building Blocks applies?

Using False Positive Building Blocks:

A. helps to prevent unwanted alerts, but there is no effect on performance.
B. helps to prevent unwanted alerts, and reduces the performance impact of testing rules that do not need to be tested.
C. has no impact on unwanted alerts, but it does reduce the performance impact of testing rules that do not need to be tested.
D. has no impact on unwanted alerts, or performance.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-Understanding-Eliminating-Unwanted-Alerts/ta-p/44924

QUESTION 18
An auditor has requested a report for all Offenses that have happened in the past month. This report generates at the end of every month but the auditor needs to have it for a meeting that is in the middle of the month.

What will happen to the scheduled report if the analyst manually generates this report?

A. The scheduled report needs to be reconfigured.
B. The analyst needs to delete the scheduled report and create a new one.
C. The report will get duplicated so the analyst can then run one manually.
D. The report still generates on the schedule initially configured.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Shared schedules must be deleted manually using the Schedules page in the web portal or the Shared Schedules folder in Management Studio. If you delete a shared schedule that is in use, all references to it are replaced with reportspecific schedules.
If you delete a shared schedule that is used by multiple reports and subscriptions, the report server will create individual schedules for each report and subscription that previously used the shared schedule. Each new individual schedule will contain the date, time, and recurrence pattern that was specified in the shared schedule. Note that Reporting Services does not provide central management of individual schedules. If you delete a shared schedule, you will now have to maintain the schedule information for each individual item.

Reference: https://docs.microsoft.com/en-us/sql/reporting-services/subscriptions/create-modify-and-delete-schedules?view=sql-server-ver15

QUESTION 19 An analyst needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter
B. List of test conditions
C. Rule actions
D. Rule responses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.
How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Navigate, and then Destination Summary
B. Right-click on the destination address, More Options, then IP Owner
C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup
D. Right-click on the destination address, More Options, then Information, and then DNS Lookup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Navigate > View Destination Summary Displays the offenses that are associated with the selected destination IP address.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

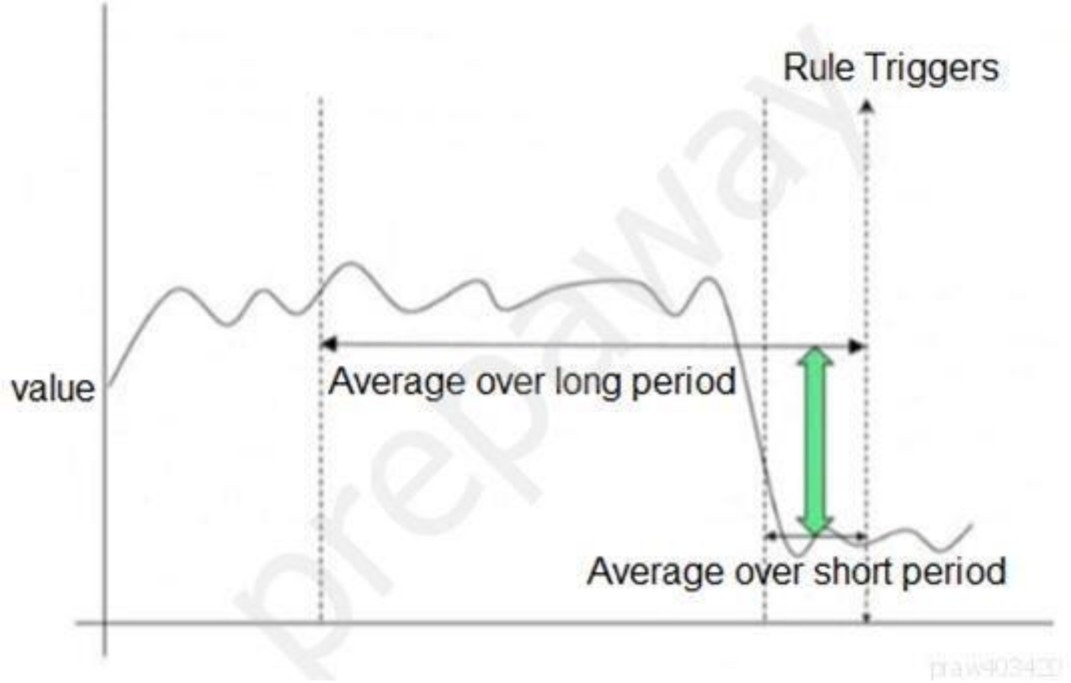
QUESTION 21 Which filter would an analyst apply in the Log Activity tab to get a list of log sources not reporting to QRadar?

A. Log source status does not equal active
B. Custom rule equals device stopped sending events
C. Log source type does not equal active
D. Log source status does not equal error

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
The graph below shows a time series of a value. A rule has been created which will trigger at the indicated point.



Which type of QRadar rule has been used?

A. Common Rule
B. Threshold Rule
C. Behavioral RuleD. Anomaly Rule

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
When an Offense is triggered, it only shows the events that triggered the Offense. The analyst wants to investigate further to see more events around the incident, not only those that triggered the Offense. The analyst clicks on the event count and sees the events belonging to the Offense.

How can the analyst proceed to see a more detailed picture of what occurred?

A. Right-click on the source IP, and choose More Options, then Information, and then Search Events.
B. Right-click on the destination IP, and choose More Options, then Raw Events.
C. Right-click on the source IP, and choose View in DSM Editor.
D. Right-click and filter on the Destination IP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=events-filtering

QUESTION 24 While creating a new custom property, which is a valid property type selection?

A. Flow Based
B. Event Based
C. AQL Based
D. Regular Expressions Based

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25 How many normalized timestamp field(s) does an event contain?

A. 2
B. 3
C. 4
D. 1

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

Explanation:
There are 3 timestamp fields on events in Qradar.

Reference: https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-different-time-stamps-for-qradar-events?language=en_US

QUESTION 26 What is the intent of the magnitude
of an offense?

A. It measures the age of the event attached to the offense.
B. It measures the age of the offense.
C. It measures the importance of the offense.
D. It measures the importance of the event attached to the offense.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The age of the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization

QUESTION 27 What is the purpose of Anomaly
detection rules?

A. They inspect other QRadar rules.
B. They detect if QRadar is operating at peak performance and error free.
C. They detect unusual traffic patterns in the network from the results of saved flow and events.
D. They run past events and flows through the Custom Rules Engine (CRE) to identify threats or security incidents that already occurred.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/topics/concept/concept-jsa-user-anomaly-detection-rules.html#:~:text=Anomaly%20detection%20rules%20test%20the,patterns%20occur%20in%20your%20network.&text=Typically%20the%20search%20needs%20to,%2C%20thresholds%2C%20or%20behavior%20changes

QUESTION 28
What could be a possible reason that events are routed directly to storage by the custom rule engine (CRE)?

A. System is under high load
B. A rule is processing 20,000 EPS
C. Event normalization issue
D. Event Parsing issue

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=appliances-expensive-custom-rule-found

QUESTION 29 An analyst needs to perform
Offense management.

In QRadar SIEM, what is the significance of “Protecting” an offense?

A. Escalate the Offense to the QRadar administrator for investigation.
B. Hide the Offense in the Offense tab to prevent other analysts to see it.
C. Prevent the Offense from being automatically removed from QRadar.
D. Create an Action Incident response plan for a specific type of cyber attack.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Protecting offenses:
You might have offenses that you want to retain regardless of the retention period. You can protect offenses to prevent them from being removed from QRadar after the retention period has elapsed.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 30 Which consideration should be given to the position of rule tests that evaluate regular expressions (Regex tests)?

A. They can only be used in Building Blocks to ensure they are evaluated as infrequently as possible.
B. They are usually the most specific. As such, they should appear first in the order.
C. They are usually the most expensive. As such, they should appear last in the order.
D. They are stateful tests. As such QRadar automatically evaluates them last.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://towardsdatascience.com/everything-you-need-to-know-about-regular-expressions-8f622fe10b03

QUESTION 31 Where can an analyst working with Offenses add a regular expression test into an existing rule?

A. Left
B. Top
C. Bottom
D. Right

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 An analyst for a particular offense needs to investigate to understand the breakdown of the offense details.

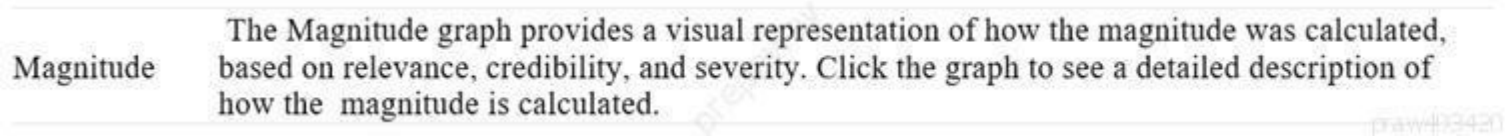
How can the analyst do this?

A. Look at the magnitude information and its breakdown.
B. Look at all the event QIDs attached to the offense.
C. View the attack path of the offense.
D. Look at the list of categories, event low level categories and the events attached.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:



Magnitude	The Magnitude graph provides a visual representation of how the magnitude was calculated, based on relevance, credibility, and severity. Click the graph to see a detailed description of how the magnitude is calculated.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=offenses-offense-investigation

QUESTION 33 An analyst has to perform an export of events within a timeframe, but not all the columns are present in the log view for the time period the analyst has selected. The analyst only needs specific columns exported for an external analysis.

How can the analyst accomplish this task?

A. Edit the search and select the extra columns, then export the result with Action/Export to XML/Full Export. This export is only supported in XML.
B. Edit the search and select the extra columns, then export the result with Action/Export to XML/Visible Columns. This export is only supported in XML.
C. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/Full Export.
D. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/Visible Columns.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-exporting-events

QUESTION 34 An analyst aims to improve the detection capabilities on all the Offense rules. QRadar SIEM has a tool that allows the analyst to update all the Building Blocks related to Host and Port Definition in a single page.

How is this accomplished?

A. Admin –> Reference Set management
B. Assets –> Asset Profiles
C. Assets –> Server Discovery
D. Admin –> Asset Profile Configuration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35 What information is included in flow details but is not in event details?

A. Log source information
B. Number of bytes and packets transferred
C. Network summary information
D. Magnitude information

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Explanation:
Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network sessions between two hosts. Reference:

https://www.ibm.com/docs/en/qsip/7.3.2?topic=overview-qradar-events-flows

QUESTION 36 An analyst had been researching an Offense that has now disappeared from the active Offense list.

What is the period of time that has to pass before an active Offense that receives no new contributing events or flows become inactive?

A. 5 days
B. 3 days
C. 24 hours
D. 1 hour

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the five-day counter is reset.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 37
An analyst needs to find all events that are creating offenses that are triggered by rules that contain the word suspicious in the rule name.

Which query can the analyst use as a working sample?

A. SELECT LOGSOURCETYPE(logsourceid), “from log_events whereRULENAME(creeventlist) ILIKE ‘%suspicious%’
B. SELECT LOGSOURCERULES(logsourceid), “from rule_events whereRULENAME(creeventlist) ILIKE ‘%suspicious%’
C. SELECT LOGGEDOFFENSE(logsourceid), *from offense_events whereRULENAME(creeventlist) ILIKE ‘%suspicious%’
D. SELECT LOGSOURCENAME(logsourceid), * from events whereRULENAME(creeventlist) ILIKE ‘%suspicious%’

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-advanced-search-options

QUESTION 38 There are 5 authentication servers that report to different Event Processors. There is a requirement to generate an Offense if there are 5 consecutive failed logins detected across any of the 5 Event Processors.

Which type of rule should the analyst create?

A. Global Rule
B. Persistent Rule
C. Local Rule
D. Offense Rule

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Global rules These rules use the Any domain modifier and run across all tenants.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_admin_guide.pdf

QUESTION 39
From which tab in QRadar SIEM can an analyst search vulnerability data and remediate vulnerabilities?

A. Log Activity
B. Dashboard
C. Assets
D. Admin

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
When IBM Security QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the Vulnerabilities tab. From the Assets tab, you can run IBM Security QRadar Vulnerability Manager scans on selected assets.

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 40 An analyst observed a port scan attack on an internal network asset from a remote network.

Which filter would be useful to determine the compromised host?

A. Any IP
B. Destination IP [Indexed]
C. Source or Destination IP
D. Source IP [Indexed]

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41 What is the difference between a Quick Search and an Advanced Search?

A. An Advanced Search uses a saved search, while a Quick Search uses a query language.
B. A Quick Search displays results by column, while an Advanced Search displays results by Category.
C. A Quick Search uses a saved search, while an Advanced Search requires a query language.
D. An Advanced Search displays results by Category, while a Quick Search displays results by column.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Quick Search

Use the search box to quickly find documents by any keyword or criteria. Here you can also view and re-use your most recent and saved searches.

Advanced Searching
The advanced search allows you to build structured queries using the Jira Query Language.

Reference: https://support.netdocuments.com/hc/en-us/articles/206955786-Quick-Search https://confluence.atlassian.com/jirasoftwareserver/advanced-searching-939938733.html

QUESTION 42 An analyst needs to map a geographic location on all the internal IP addresses.

Which option defines the functions where the analyst can-setup a geographic location of the network object in Network Hierarchy?

A. GPS location and Map
B. Group and IP address
C. Log Activity and Network Activity
D. Longitude and Latitude

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy

QUESTION 43
An analyst needs to review additional information about the Offense top contributors, including notes and annotations that are collected about the Offense.

Where can the analyst review this information?

A. In the top portion of the Offense Summary window
B. In the bottom portion of the Offense main view
C. In the bottom portion of the Offense Summary window
D. In the top portion of the Offense main view

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the bottom portion of the Offense Summary window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using-summary-information

QUESTION 44
An analyst is investigating a user’s activities and sees that they have repeatedly executed an action which triggers a rule that emails the SOC team and creates an Offense, indexed on Username.

The SOC team complained that they have received 15 emails in the space of 10 minutes, but the analyst can only see one Offense in the Offenses tab.

How is this explained?

A. There is a Rule Limiter on the Rule Action which creates the Offense, this should also be applied to the Rule Responses.
B. This is expected behavior, the offense will contain the information about all 15 events.
C. An Offense rule has been configured to send multiple emails upon Offense creation.
D. The Custom Rules Engine (CRE) has fallen behind and the additional Offenses will be created shortly.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
An analyst has observed that for a particular user, authentication to an organization's critical server is different than the normal access pattern.

How can the analyst verify that all the authentications initiated from the user are valid?

A. Perform a search with filter Destination IP group by Username, then validate the Username
B. Perform a search with filter Source IP group by Username, then validate the Username
C. Perform a search with filter Username group by Source IP, then validate the Destination IPD. Perform a search with filter Username group by Source IP, then validate the Source IP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
How does an analyst view the base64 encoded string of an event's raw payload that contains unprintable characters?

A. Copy the raw payload and use an external tool to view base64 data
B. Right click on the event –> view base64 data
C. Log Activity –> Under Payload Information, click base64 tab
D. Admin –> Under Payload Information, click base64 tab

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which QRadar component stored Offenses?

A. Console
B. Data Node
C. Event Processor
D. Event Collector

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
QRadar Data Node
Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Nodes help to increase the search speed in your deployment by providing more hardware resources to run search queries on.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=overview-qradar-components

QUESTION 48
The administrator had set up several scheduled reports that can be executed by analysts every Monday, and the first day of each month. On Thursday, an executive requests one of the weekly reports.
If the analyst executes the report on Thursday, what information will the report contain?

A. Data from Monday to Sunday from the previous week.
B. Data from Thursday from the previous week to Wednesday from the current week.
C. Data from Monday to Thursday from the current week.
D. Data from Monday to Wednesday from the current week.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
An analyst is investigating a series of events that triggered an Offense. The analyst wants to get more detailed information about the IP address from the reference set.

How can the analyst accomplish this?

A. Click on Searches tab then perform an Advanced Search
B. Click on Log Activity tab then perform a Quick Search
C. Click on Searches tab then perform a Quick Search
D. Click on Log Activity tab then perform an Advanced Search

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 What does the Assets tab provide?

A unified view of the information that is known about:

A. network devices.
B. triggered Offenses.
C. log sources.
D. events and flows.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/identity-and-how-log-source-events-update-assets-qradar-siem

QUESTION 51 An analyst needs to find events coming from unparsed log sources in the Log Activity tab.

What is the log source type of unparsed events?

A. SIM Generic
B. SIM Unparsed
C. SIM Error
D. SIM Unknown

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SIM Generic log source or by using the Event is Unparsed filter.

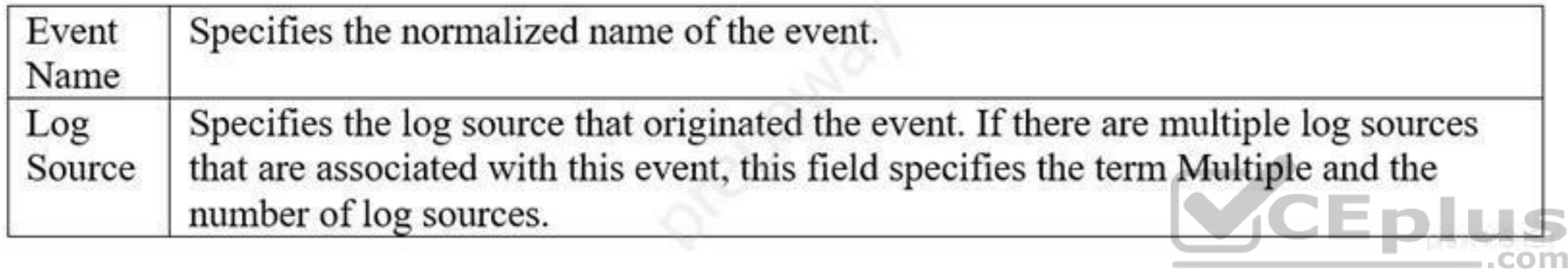
Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

QUESTION 52 What information is displayed in the default “Log Activity” page?
(Choose two.)

A. QID
B. Protocol
C. Qmap
D. Log Source
E. Event Name

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
By default, the Log Activity tab displays the following parameters when you view normalized events:



Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.

Reference: https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-users-guide/topics/concept/concept-jsa-user-log-activity-monitoring.html

QUESTION 53 Which are the supported protocol configurations for Check Point integration with
QRadar? (Choose two.)

A. CHECKPOINT REST API
B. SYSLOG
C. JDBC
D. SFTP
E. OPSEC/LEA

Correct Answer: BE
Section: (none)
Explanation

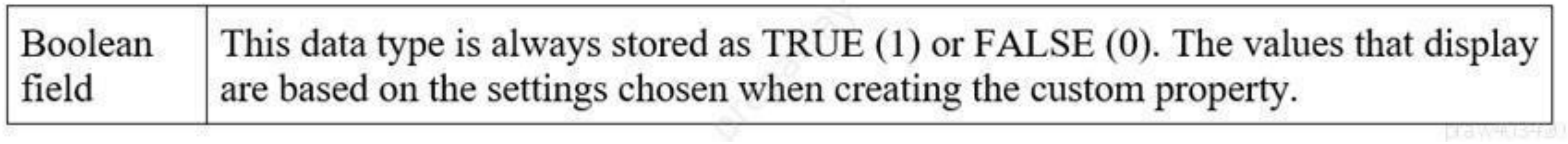
Explanation/Reference:

QUESTION 54 An analyst needs to use a new custom
property in a rule.

What must be the mandatory characteristic of the custom property?
A. It must be shared.
B. It must be boolean.
C. It must be stored.
D. It must be extracted.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:



Boolean field	This data type is always stored as TRUE (1) or FALSE (0). The values that display are based on the settings chosen when creating the custom property.

Reference: https://kb.wisc.edu/ecms/page.php?id=34358

QUESTION 55 What is the procedure to re-open a closed Offense?

A. A closed Offense cannot be re-opened.
B. Wait for new events/flows that will re-open the closed Offense.
C. Activate the Offense in the action/re-open drop down menu of the Offense tab.
D. Activate the Offense in action/re-open drop down menu in the Admin tab.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Not possible to reopen a closed offense.

Reference: https://www.ibm.com/support/pages/qradar-closed-offense-information

QUESTION 56 An analyst wants to view information about repeated offenders and IP addresses that generate many attacks or are subject to many attacks.

What should the analyst choose from the navigation options in the Offense tab?

A. By Event Category or By Event Source
B. By Source IP or By Destination IP
C. By Log Source IP or By Event Source
D. By Event or By Flows

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Use the navigation options on the left to view the offenses from different perspectives. For example, select By Source IP or By Destination IP. Reference:

https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 57
An analyst needs to perform a Quick search to find events under the Log Activity tab that contains an ‘exe’ file during a certain time period.

How can the analyst do this?

A. On the Search bar select Quick Filter, then insert filter criteria for ‘/*.exe/’ and then select a time interval from the view option’s drop down.

B. Select Search – New Search from the menu bar, then select all the search criteria required from the UI options provided.
C. Select Quick Searches on the menu bar, then go through the list of saved searches available to see if one already exists, that can be altered.
D. On the Search bar select Quick Filter, insert: ‘exe, last 1 hour’ into the filter criteria, then click Search.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters

QUESTION 58 What is a valid offense naming mechanism?

This information should:

A. set the naming of the associated offense(s).
B. set or replace the naming of the associated offense(s).
C. replace the naming of the associated offense(s).
D. be included in the naming of the associated offense(s).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Under "Offense Naming", check "This information should contribute to the name of the associated offense(s)".

Reference: https://www.ibm.com/support/pages/apar/IJ27086

QUESTION 59 What are the different flow types in QRadar?

A. L2L, L2R, R2R, R2L
B. Standard, Type A, Type B, Type C
C. Standard, Type 1, Type2, Type 3
D. Type 1, Type 2, Type 3, Type 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docplayer.net/19071559-Qradar-siem-7-2-flows-overview.html

QUESTION 60 An analyst needs to investigate why an Offense was created.

How can the analyst investigate?

A. Review the Offense summary to investigate the flow and event details.
B. Review the X-Force rules to investigate the Offense flow and event details.
C. Review pages of the Asset tab to investigate Offense details.
D. Review the Vulnerability Assessment tab to investigate Offense details.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference: